GIFTS: Ethical or Not?: A Mock Jury Duty Activity for Establishing a Foundational Ethical Framework in Early Cybersecurity Education

Ian Hong Phan, University of California, Santa Cruz

Ian Phan is a current Graduate Student in Human-Computer Interaction at the University of California, Santa Cruz. He has been involved with the Early Design Experiences program at UC Santa Cruz's Baskin School of Engineering for three years, serving as a student instructor and coach for teaching teams developing new courses. His work focuses on advancing collaborative STEM education, promoting interdisciplinary collaboration, and reducing barriers to success in engineering fields. Beyond the classroom, his involvement in mentoring and volunteering for high school robotics, as well as conducting research on participatory programs expanding undergraduate research and learning opportunities, further strengthens his commitment to fostering inclusive and accessible educational opportunities. Through his work, he aims to foster curiosity, collaboration, and confidence among all students, preparing them to tackle complex, real-world challenges.

Iakov Taranenko, University of California, Santa Cruz

Iakov Taranenko is a recent graduate in computer networking at the University of California, Santa Cruz. For three years, he served as a student instructor for a first year design program specializing in cybersecurity, helping underclassmen explore the cybersecurity field. Extremely passionate about cybersecurity, he brings valuable knowledge from his employment as a systems exploitation engineer within government roles and his participation in graduate-level cybersecurity research. This experience extends beyond his academic work into student leadership, where as president of the university's cybersecurity student organization, he organizes hands-on workshops, mentors team members for national cybersecurity competitions, and creates opportunities for students to test their hacking skills against realistic simulated systems. Under his leadership, the club has significantly increased membership and regularly places among the top teams in collegiate cybersecurity challenges across the country.

Dr. Tela Favaloro, University of California, Santa Cruz

Tela Favaloro is an associate teaching professor for the Baskin School of Engineering at UCSC where she works to establish holistic interdisciplinary programming centered in experiential learning. Her Ph.D is in Electrical Engineering with emphasis in the design and fabrication of laboratory apparatus and techniques for electro-thermal characterization of sustainable power systems as well as the design of learner-centered experiential curriculum. She is currently working to develop an inclusion-centered first-year engineering program in hands on design and problem-based learning to better support students as they enter the engineering fields.

GIFTS: Ethical or Not? A Mock Jury Duty Activity for Establishing a Foundational Ethical Framework in Early Cybersecurity Education

This GIFT describes *Jury Duty*, an interactive collaborative classroom activity which expands upon the traditional engineering ethics lecture to supply early-career students with a structured ethical framework that they may apply to cybersecurity or other complex scenarios.

Motivation

A persistent challenge in cybersecurity education is moving students beyond the simplistic *black* vs *white hat* view of hacking [1]. While the distinction between these groups is often defined by intent, the ethical underpinning of the hacking community is far more complex. Central to this professional landscape is the concept of ethical hacking, where professionals deliberately breach systems for the sole purpose of identifying and remediating vulnerabilities [1].

However, while students are naturally drawn to the high-stakes technical challenges of the field, they are often ill-equipped to make defensible ethical judgements due to the lack of a solid foundational framework [2, 3, 4, 5]. Standard ethics instruction often relies on passive instruction, such as lecture or memorization of professional ethics codes or legal frameworks. These approaches fail to adequately prepare students for the messy scenarios, ambiguities, and ethical gray areas inherent in professional practice [3, 6]. The conceptual gap between learning and practice is exacerbated by instruction that is skills-focused and thus "offensive" first, which while highly motivating, frames hacking as simply a "collection of tricks" rather than a disciplined professional practice [2].

These issues are prevalent in current cybersecurity and other engineering curricula. Addressing them drove the creation of this GIFT, which fosters practical wisdom by bringing students into the micro-macro ethical divide – the link between one's choices and their broader societal consequences [3, 6]. *Jury Duty* achieves this through a collaborative mock-jury format that situates students both individually and in groups as the primary evaluators of ethically ambiguous cases. In doing so, we transform abstract theory into a practical toolkit, required to navigate the professional field, achieving the recommendations from [7].

Objectives

The *Jury Duty* activity translates the theoretical needs of the engineering curriculum into a structured, shared experience, with the goal of shifting students away from forming a simple, intuitive "gut feeling" about hacking ethics towards a more rigorous, professional analysis. The activity is designed around three core learning outcomes, where students will be able to:

- Identify and apply a multi-faceted framework for evaluating the ethics of actions taken in cybersecurity/hacking to move beyond a binary "black hat/white hat" worldview.
- Analyze complex, ambiguous scenarios to formulate and defend an ethical position that can withstand both group deliberations and external pressure.
- Articulate the distinction between personal judgement, group consensus, and legal requirements in ethical decision-making to bridge the micro-macro ethical divide.

- Recognize that a technically proficient or personally moral action may still violate broader professional norms or legal standards.

Ultimately, this activity offers instructors a practical instructional blueprint for moving beyond passive lectures on a complex topic like ethics. Rather than seeing hacking as a fragmented "collection of tricks," students must reconcile their technical choices with the legal and ethical standards required of disciplined professional practice, promoting a sense of responsibility for the impact of their work. Thus, *Jury Duty* provides a durable foundation for students' future careers and satisfies the recommendations laid out in [2, 4].

Implementation

Jury Duty is a ~95 minute in-class activity delivered early in the curriculum of an introductory cybersecurity course [8] to move ethics from a passive lecture into a shared, active experience. The activity is grounded in Kolb's model of experiential learning, where deep learning occurs through a cycle of concrete experience, reflective observation, abstract conceptualization, and active experimentation [7, 9]. By placing students in the role of jurors, the activity provides a *concrete experience* that demands decision making, *active experimentation* through negotiation, a structure requiring students to engage in *reflective observation* of the conflicting evidence in the cases, and *abstract conceptualization* of how professional standards apply to various situations in hacking and cybersecurity.

1. Pre-Instruction: Establishing the Ethical Toolkit (slide-based discussion ~30 minutes)
To prepare students for the mock-jury activity, we provide a foundational toolkit that establishes common language and the evaluative criteria. This stage is critical for moving students beyond the simplistic views of cybersecurity towards a more nuanced professional understanding.

The instruction begins with a blunt reminder of the legal landscape surrounding cybersecurity with the *Don't Get Arrested* slide (Appendix A), which serves to immediately ground the discussion in the high stakes reality of the field. Here, we introduce federal and state legal frameworks: Computer Fraud and Abuse Act (18 U.S.C. § 1030) and California Penal Code 502(c) to illustrate the immediate consequences of unauthorized access [10, 11]. This segment of the activity emphasizes that technical curiosity alone is not a legal defense and introduces the concept of professional self-regulation before any technical skills are practiced (we present this activity on the second day of class). By framing the lecture around personal and professional risk, we shift the students' focus from what they *can* do to the legal boundaries of what they *should* or *may* do.

Students are then introduced to the primary *types* of hackers, distinguished by their motivation and relationship to authority: ***White Hats*** protect systems or conduct security testing with consent, ***Black Hats*** operate maliciously and cause harm, while ***Gray Hats*** occupy an ambiguous middle ground, lacking malicious intent but also explicit authorization. We navigate this ambiguity using a five-point evaluative framework which functions as a field-specific "code of conduct" for deliberation: **Authorization, Intent, Methods, Disclosure,** and **Legality** (Appendix B). Students are asked to evaluate a hacker's actions across these dimensions; thus, they together serve as a necessary toolkit. However, ethics often depend heavily on personal judgement. As such, this toolkit is intended primarily as a launching pad for students to form

their own independent arguments, forcing students to move beyond passive rule-memorization and instead weigh competing values to reach their own defensible conclusions.

2. Case Study Application (worksheet-based group discussion ~60-65 minutes)

The next stage of the activity is *concrete experience*, where the toolkit is applied through a mock-jury activity. Learners are placed into small groups of 'jurors' where they deliberate on real-world scenarios using the 5-point framework as a scaffold. These scenarios are intentionally selected to be two-sided, where arguments can be made and are encouraged for both sides of the ethical spectrum. In our implementation, we curated the following scenarios for analysis as they touch on multiple points of the framework: a rental bicycle systems exploit, a course gradebook grade-change incident, and a data privacy vulnerability in a ticket reporting system (Appendix C). The following is how our implementation plays out in class:

1. **Case Study Introduction and Overview**: We first introduce a case study and ask students to consider the framework when discussing the nature of the defendant's actions.
2. **Deliberation**: Students are given 10 minutes to "deliberate" in a group of 3 - 4. They utilize the *Hacking Ethics Worksheet* (Appendix D) to reach a conclusion of guilty/not guilty across the 5 counts (listed above). Note the worksheets prompts learners to record both the group consensus and their individual verdict.
3. **Class Discussion**: After deliberations, each student-group shares out their overall ruling of the case, citing the specific counts that contributed towards their final decision.

We repeat these three steps above for the next two case studies so that students are exposed to a variety of scenarios yet utilize the same framework to guide their thinking. Students are not just choosing *guilty* or *not guilty* on each of the five counts but are instead evaluating the specific ethical and legal dimensions of the hacker's actions to reach a more well-rounded final decision, moving from passive absorbers of rules to active participants in professional ethical reasoning.

3. Reflection

After the class session concludes, students take the worksheet as homework where they are asked to individually reflect on each scenario analyzed in class. Here, learners are prompted to explicitly consider uncertainty in their judgement and prioritize the ethical principles that helped them draw their conclusions. This reflection aids in solidifying the student's transition from a singular experience to a generalized professional mindset. By evaluating their personal verdicts and opinions against the group's, students move from *reflective observation* of the activity towards *abstract conceptualization*, where they begin to synthesize their own internal ethical standards for future professional practice.

Assessment

The effectiveness of this GIFT is evaluated through observation during in-class discussions and a thematic analysis of student submissions via the Hacking Ethics Worksheet. Rather than grading students on the "correctness" of their verdicts, our focus is on making student-thinking visible by measuring progress towards the core learning outcomes established in the objectives. The primary data for these evaluations are derived from the individual reflection prompts, which provide tangible evidence of student growth in professional reasoning.

By requiring students to first consider their own verdict, then discuss with their fellow 'jurors' and deliver verdicts across the five counts for each case study, the worksheet surfaces their ability to apply the multi-faceted framework to a variety of scenarios. Observations from four distinct implementations across different student cohorts show that learners consistently internalize this language, opting to use professional terminology rather than subjective opinion in their justifications. For example, one student noted that while the perpetrator's intent seemed like curiosity, they were still "*guilty, but [defendant] would get a small fine at most.*" Another student used technical nuance as justification, arguing the individual was "*only guilty of unauthorized access because [defendant] went a step further to create a script that scrapes this data.*"

Furthermore, the final reflection prompt unpacks students' uncertainty on specific "counts" in play, forcing them to articulate the rationale behind their decisions in complex, ambiguous scenarios, with responses indicating that students successfully synthesized conflicting evidence, particularly in cases where the perceived moral outcome and legal standards are at odds. One student noted that a scenario "*started out unethical then became ethical in the end, however, it was difficult to decide if guilty or not when [defendant] disclosed it afterwards.*" Another student admitted difficulty judging actions that mirrored themselves, stating, "*because this case seems like something that I would do, it ethically felt harder for me to [reach a] verdict [of] guilty.*"

Perhaps the most significant result is the evidence of independent moral agency. By comparing their personal verdicts to the group consensus, students bridge the micro-macro ethical divide to recognize that a personally moral action may still violate professional norms, even amongst their own peers. In the most recent iteration of the activity, all submissions showed at least one point of divergence between the individual and group verdicts, indicating the students' ability to maintain a defensible position, a vital competency for upholding ethical standards against external pressure. This resistance was captured by a student who maintained a "not guilty" verdict, explaining "*I can totally understand why my groupmates voted guilty on everything… [but] I interpreted it as irresponsible disclosure but an unintended thing.*" Another student also reached a less harsh personal verdict than their group, reasoning the perpetrator had "*reported the issue with only a mild infraction, [defendant should] be given more leniency.*"

Ultimately, these results indicate that the activity successfully provides students with a practical toolkit for navigating the ethical complexities of cybersecurity. By the conclusion of the activity, students gain a newfound perspective of hacking as not just a fragmented "collection of tricks," but move towards seeing it as a disciplined and responsible professional practice requiring constant self-regulation to the legal and ethical standards of the cybersecurity community.

Conclusions

By situating learners within a collaborative mock-jury format, our GIFT *Jury Duty*, experientially transforms ethics from an abstract, passive lecture into a practical toolkit that moves students beyond the binary *black/white hat* view towards a more sophisticated understanding of ethical hacking as a regulated professional practice. Results over multiple implementations show students not only internalized the language of professional accountability, but also developed the critical thinking skills necessary to navigate the gray areas of the field. This activity's framework provides a durable foundation for students to view their skills developed later in the course and beyond through a lens of disciplined professional practice.

References

[1] B. CP, “Analysis of white and black hat hacker roles, practices and techniques, considering ethical and legal issues, including Bug Bounty programs,” SunText Review of Economics & Business, vol. 04, no. 04, 2023. doi:10.51737/2766-4775.2023.095

[2] T. Hynninen, “Student Perceptions of Ethics in Cybersecurity Education,” Conference on Technology Ethics, pp. 79–93, 2023.

[3] J. Blanken-Webb, I. Palmer, S. E. Deshaies, N. C. Burbules, R. H. Campbell, and M. Bashir, ‘A Case Study-based Cybersecurity Ethics Curriculum’, in 2018 USENIX Workshop on Advances in Security Education (ASE 18), 2018.

[4] A. Hingle and A. Johri, “A framework to develop and implement role-play case studies to teach responsible technology use,” IEEE Transactions on Technology and Society, vol. 5, no. 3, pp. 306–315, Sep. 2024. doi:10.1109/tts.2024.3408085

[5] M. Benitz, “Strengthening undergraduates’ appreciation of engineering ethics through a simulated stakeholder meeting on offshore wind energy development,” 2023 ASEE Annual Conference & Exposition Proceedings, 2023. doi:10.18260/1-2--44276

[6] A. Hingle and A. Johri, “Role-play case studies to teach computing ethics: Theoretical foundations and practical guidelines,” Proceedings of the Annual Hawaii International Conference on System Sciences, 2024. doi:10.24251/hicss.2024.620

[7] J. Miller and T. Seidler, “Using a mock trial: An experiential learning opportunity,” Sport Management Education Journal, vol. 14, no. 1, pp. 58–60, Apr. 2020. doi:10.1123/smej.2019-0020

[8] I. H. Phan, I. Taranenko, and T. Favaloro, “Hacking the system: A peer-led cybersecurity course for early-career university students,” 2025 ASEE Annual Conference & Exposition Proceedings, 2025. doi:10.18260/1-2--56679

[9] D. A. Kolb, “Structural Foundations of the Learning Process,” in Experiential Learning: Experience as the source of Learning and Development, 2nd ed, 2015, pp. 65–87

[10] U.S. Congress, "Computer Fraud and Abuse Act," 18 U.S.C. § 1030 (2018).

[11] California Penal Code, § 502(c), California, 2019.

Appendix A: Orientating Slide Materials

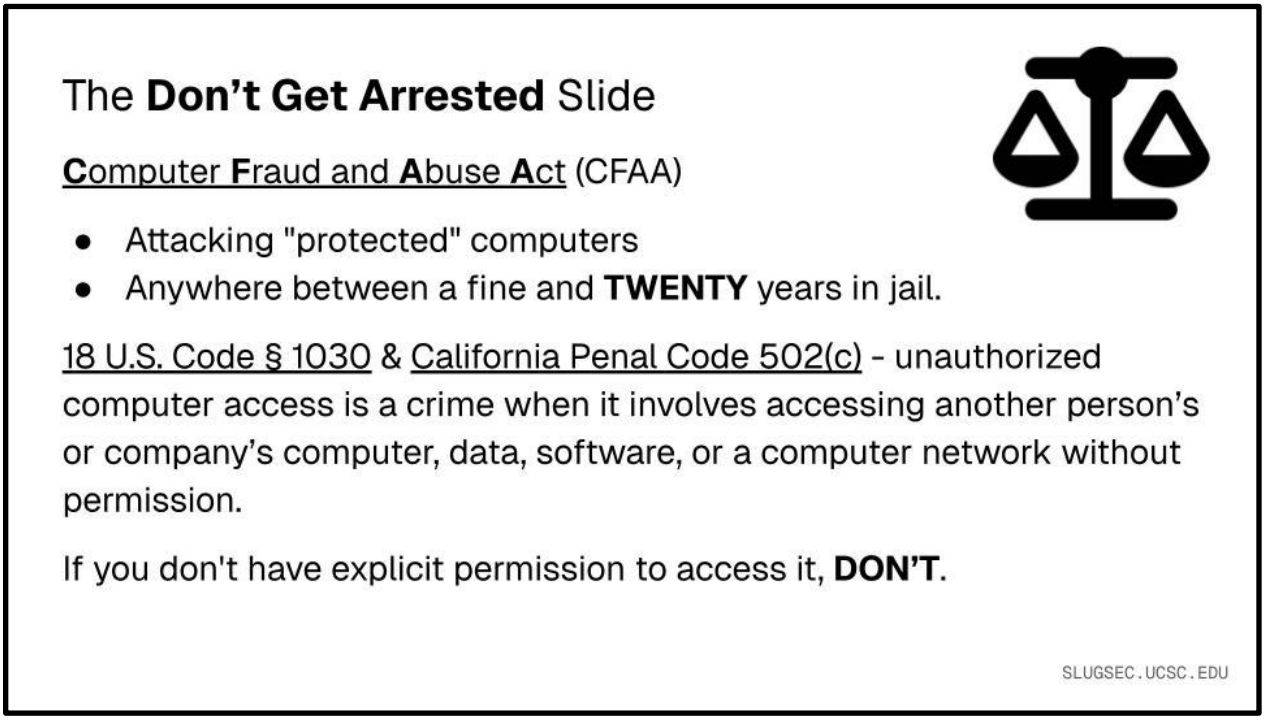


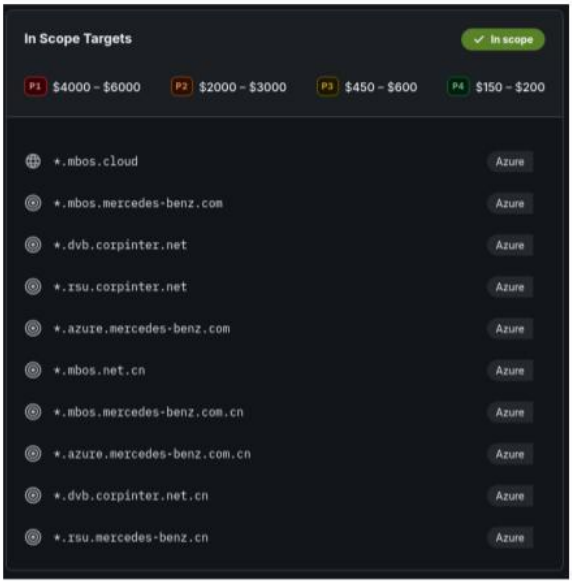
Figure 1: *The "Don't Get Arrested" slide - used throughout the course to establish legal boundaries through the Computer Fraud and Abuse Act (CFAA) and California Penal Code 502(c). By explicitly outlining the risks of twenty-year jail sentences for unauthorized access, the activity integrates legal ethics directly into the technical curriculum, ensuring students understand the real-world consequences of engineering without permission.*

Appendix B: Hacking Ethics Five-Point Framework

1. Authorization

Did you have permission before you touched anything?

Bug bounty programs, signed scope docs, pentest contracts. Authorization can also be scoped, meaning you might have permission to test a company's web app but not their internal network. Going outside your scope is the same as having no authorization at all.



SLUGSEC.UCSC.EDU

1. Authorization - Examples

Ethical:

- **Hack the Pentagon (2016)**
  DoD invited 1,400 hackers to attack their public systems. 138 valid vulnerabilities reported
- **HackerOne / Bugcrowd programs**
  companies publish scope, rules, and payouts. You find bugs within the rules, you get paid

Unethical:

- **Ahmed Al-Khabaz / Dawson College (2013)**
  CS student found a vulnerability in his college's student portal that exposed 250,000 students' personal data including social insurance numbers. Reported it, it got patched. Two days later he ran a vulnerability scanner to verify the fix. Expelled by a 14-1 faculty vote for "unauthorized access"

Who can think of more examples?

SLUGSEC.UCSC.EDU

(a)

2. Intent

What were you trying to accomplish?

This is the black/grey/white hat split. A pentester who finds a database full of credit cards and reports it has different intent than one who copies them to a flash drive. Intent matters even when you're authorized.

FBI wanted bulletin for a Chinese Advanced Persistent Threat (APT) group.

SLUGSEC.UCSC.EDU

2. Intent - Examples

Ethical:

- **Marcus Hutchins, MalwareTech (2017)**
  WannaCry was spreading across 150 countries, hitting hospitals, telecom companies, and government systems. Hutchins reverse-engineered the malware, found a kill switch domain hardcoded in it, registered it for $10.69. He didn't even know it would stop the attack, he was just sinkholing the domain to track infections.

Unethical:

- **Uber "God View" (2014)**
  Employees had legitimate access to Uber's internal tracking systems. Used it to follow journalists, politicians, and ex-partners around the city.

Who can think of more examples?

SLUGSEC.UCSC.EDU

(b)

3. Methods

Did you cause unnecessary damage along the way?

You're testing a web app for SQL injection and you accidentally drop a production database of customer records. You run an aggressive network scan and take down a company's services during business hours. You deploy a proof of concept that spreads beyond the target system. The vulnerability might be real but your methods caused harm that didn't need to happen.

Claude, I said find the SQL vulnerability and make NO MISTAKES!!

3. Methods - Examples

Ethical:

- **Charlie Miller & Chris Valasek (2015)**
  Remotely hacked a Jeep Cherokee through the Uconnect entertainment system's cellular connection. Could kill the engine and disable brakes remotely, control steering at low speeds. Gave Chrysler about nine months notice before publishing at Black Hat. Chrysler recalled 1.4 million vehicles.

Unethical:

- **Robert Morris, the Morris Worm (1988)**
  Grad student who wanted to measure how big the internet was. Wrote a self-replicating worm to do it. A bug in his code caused it to re-infect machines over and over, crashing 6,000 systems, about 10% of the entire internet.

Who can think of more examples?

(c)

4. Disclosure

Did you report what you found?

Coordinated disclosure means giving the vendor a window to patch (usually 90 days) before going public. You find a critical auth bypass in a hospital's patient portal, you don't tweet about it, you contact them and give them time to fix it. What you do with the information after you find it matters as much as how you found it

John Hammond on stage at DEFCON for HackerJeopardy
Credit @_johnhammond via X

4. Disclosure - Examples

Ethical:

- **Dan Kaminsky (2008)**
  found a fundamental flaw in DNS that would let anyone redirect internet traffic. Instead of publishing, he quietly coordinated a massive secret patching effort across every major DNS vendor simultaneously. Held off on details until Black Hat to give the patches time to roll out.

Unethical:

- **Chris Roberts (2015)**
  security researcher who claimed to have accessed airplane systems through the in-flight entertainment unit on a live commercial flight. Tweeted about it mid-air. FBI met him at the gate. Whether he actually reached flight controls is disputed, but testing on a plane full of passengers and tweeting about it is not how you disclose

Who can think of more examples?

(d)

5. Legality

Are you staying within the law?

You completed your assessment and found real vulnerabilities. Now what? Publishing a detailed writeup that lets anyone replicate the attack, selling exploits on a forum, using stolen credentials to access unrelated systems crosses legal lines. "They ignored my report" is never a legal defense for dumping their database*

36-year-old Denis Emelyantsev, an alleged Russian Hacker, was arrested in Bulgaria. Credit @vxunderground via X

5. Legality - Examples

Ethical:

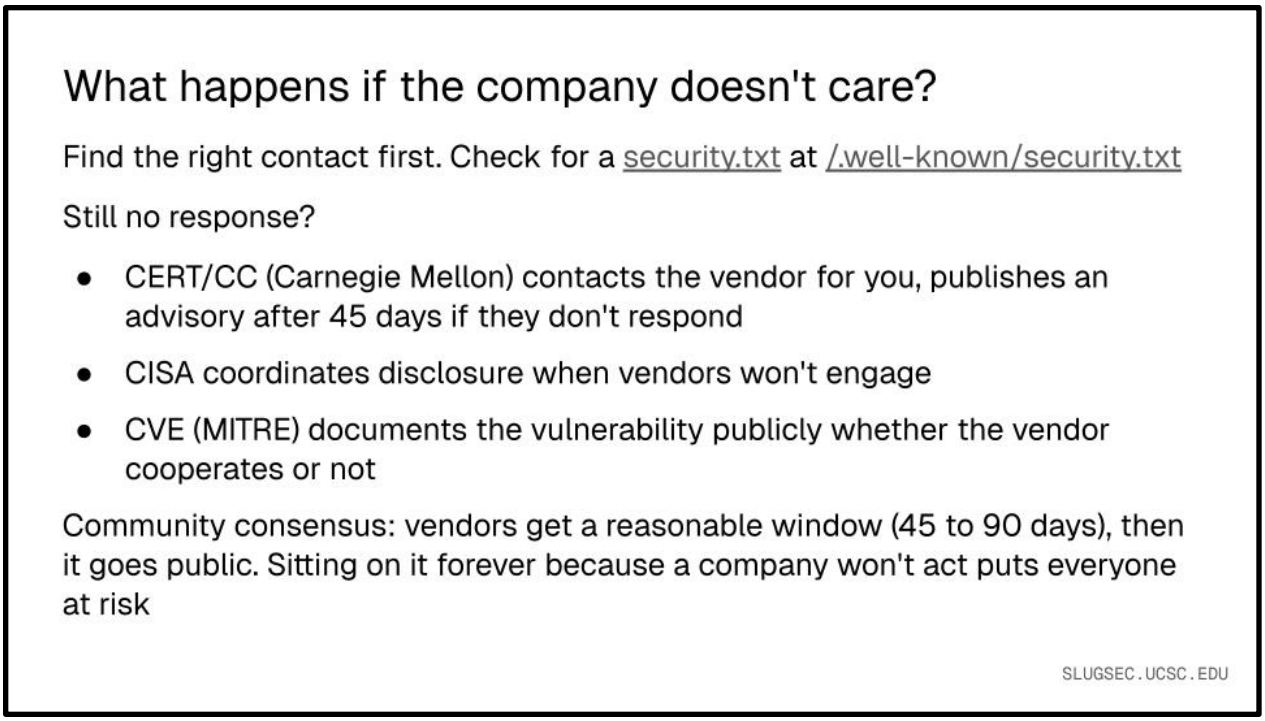
- **Katie Moussouris**
  built Microsoft's first bug bounty program, helped create Hack the Pentagon, and co-authored ISO standards for how vendors should handle vulnerability reports. Has been pushing for legal safe harbor protections for researchers for over a decade.

Unethical:

- **Matthew Keys (2010)**
  former web producer at Fox 40 in Sacramento, shared his old Tribune Company login credentials with Anonymous in an IRC chat after getting fired. They defaced a LA Times headline for about 40 minutes. Two years in prison.

Who can think of more examples?

(e)



(f)

Figure 2: *Representative instructional slides illustrating our five-point ethical framework for hacking and cybersecurity, serving as the activity's grounded programmatic code. Individual sub-figures detail the specific evaluative criteria used during student deliberations:* ***(a)*** *Authorization,* ***(b)*** *Intent,* ***(c)*** *Methods,* ***(d)*** *Disclosure, and* ***(e)*** *Legality. This modular framework is duplicated in the Hacking Ethics Worksheet (see Figure 4) to ensure a consistent instructional bridge between theoretical lecture and practical application. This portion of the slides also includes steps of recourse -* ***(f)*** *what happens if a company doesn't care? While piloted in a cybersecurity context, these dimensions are designed to be broadly adaptable to diverse engineering dilemmas, providing a structured blueprint for students to navigate the gray areas potentially encountered during professional practice.*

Appendix C: *Jury Duty* Scenario Examples

Time to use what you learned

Each table is a jury. For each case, **deliberate for 10 minutes** and **write your guilty / not guilty for each of the five pillars** on your whiteboard.

Any jury may get called up to deliver their full verdict to the class

For each scenario, rule on all five pillars:

1. Authorization did they have permission?
2. Intent were they trying to help or help themselves?
3. Methods did they break things they didn't need to?
4. Disclosure did they tell someone?
5. Legality did they stay out of jail territory?

Guilty, not guilty, or somewhere in the middle? Be ready to defend your reasoning!

Reminder: Take notes in your notebook!

SLUGSEC.UCSC.EDU

Case 1: BCycle PWNage

Last Friday, two students pwned the locking system on the rental electric bikes on campus, tricking the system into thinking bikes were checked in when they weren't.

One student then shared their methods with members of the university's cybersecurity club, who used the info to steal bicycles.

Were these students' actions ethical?
Permission? / Why? / Damage? / Report it? / Legal?

Things to consider:

- Did the students steal any bikes themselves?
- Is sharing an exploit with a group the same as using it?
- What if they had reported the vulnerability to rental company instead of the club?
- Does it matter that the people who actually stole the bikes were a separate group?

SLUGSEC.UCSC.EDU

Case 2: Canvas

A student discovered a method to log into any Canvas account associated with their university. They logged into their calculus professor's account and changed their midterm grade so they was no longer failing. After seeing it worked, they immediately contacted Canvas and the university about the vulnerability and offered to help fix it

Were this student's actions ethical?
Permission? / Why? / Damage? / Report it? / Legal?

Things to consider:

- Does reporting the vulnerability after the fact undo the grade change?
- What if they only logged in to look but never changed anything?
- What if they changed the grade and told the university what they did when they disclosed?
- They helped them fix a real security flaw. Does that matter at all for their case?
- How would this play out under the CFAA?

Case 3: Sensitive Data

A student is browsing late at night checking on their repair ticket request. They notice that they can see other people's requests, some containing PII/PHI. They builds a proof of concept, scraping a few hundred requests to document the issue. They contact the admins immediately

They say they'll fix it. Weeks go by, nothing. Months go by, nothing

Were this student's' actions ethical? What should they do now?
Permission? / Why? / Damage? / Report it? / Legal?

Things to consider:

- Did they need to scrape records to prove the point, or would a screenshot have been enough?
- They're now sitting on other people's medical and personal data. What's their responsibility with that?
- The admins know and won't act. Are they liable if someone else finds the same flaw and leaks it?
- Should they go to CERT/CC? CISA? The press? What are the tradeoffs of each?
- At what point does the company's inaction become more unethical than anything the student did?

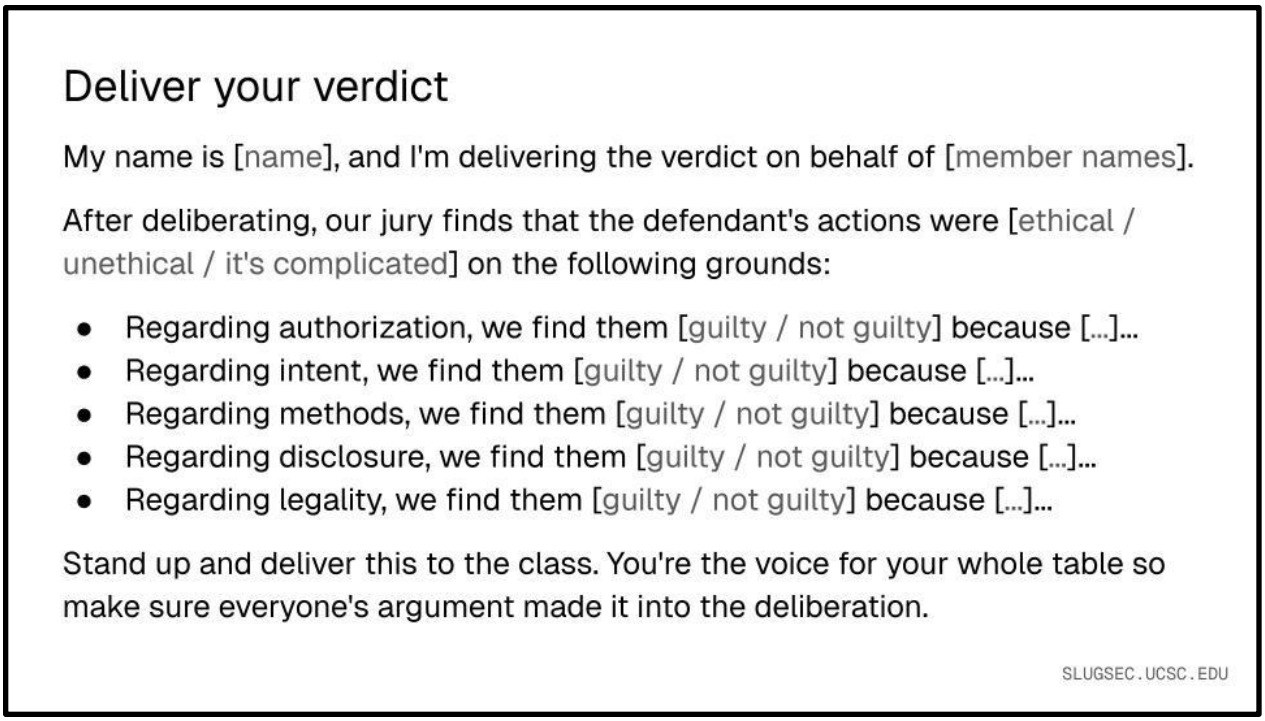


Figure 3: *Representative instructional slides for "Jury Duty," including our three curated scenarios used during the activity, as well as the "Your Rulings" prompt used to facilitate team discussions during the mock- jury process. Cases are based on both real-life and fictional scenarios, however, the focus is directed on evaluating the case against each "count" rather than the reality or the correctness of each case.*

Appendix D: Hacking Ethics Worksheet

Scenario:

_____

Team discussion notes:

_____
_____
_____
_____
_____

Count	Group Verdict	My Verdict
Unauthorized access of a computer system		
Intent to cause harm or gain unauthorized benefit		
Use of prohibited methods or tools		
Failure to disclose security vulnerabilities responsibly		
Violation of legality (CFAA/US criminal code)		

Personal reflection (do after class): Did your personal verdict differ from your group's verdict? Why or why not? What ethical principles guided your thinking? Was one more important than the other? Were there any counts where you felt uncertain, and what made them difficult to judge? ***(respond in 3-5 sentences)***

_____
_____
_____
_____
_____
_____
_____
_____

Figure 4: *Hacking Ethics Worksheet used during the "Jury Duty" activity. The table requires students to evaluate scenarios across five specific counts, while also recording both a group verdict and an individual verdict. This structure is designed to foster independent moral agency as students compare their personal reasoning against the group consensus.*